CLAIMS

1. A cryptographic method implemented by a smart card (30) of a set of smart cards each belonging to a first entity that may be different for each smart card, each smart card being equipped with a chip (31) comprising storage means (32) in which are stored a secret key and an identifier of the first entity that is the proprietor of the smart card (30) and calculation means (33) which execute a cryptographic algorithm whose input arguments include at least the secret key, which method is characterized in that it comprises the following steps:

- before any calculation by the calculation means (33) of the chip (31) of the smart card (30), the chip (31) reads in storage means of a second entity a list of identifiers in complete form of first entities that are smart card proprietors (operation 2), said list being linked to the status assigned to each of the first entities by the second entity, and

- the chip (31) compares the identifiers stored in the storage means (32) of the chip (31) and the contents of the list (operation 3) to authorize (operation 5) or prohibit (operation 4) calculation by the calculation means (33) as a function of the result of the comparison.

2. A cryptographic method according to claim 1, wherein the list comprises all first entities whose status has been set to "revoked" by the second entity and the chip (31) authorizes calculation (operation 5) only if the identifier stored in the storage means (32) of the chip (31) is not in the list.

3. A cryptographic method according to claim 1, wherein the list comprises all first entities whose status has been set to "non-revoked" by the second entity and wherein the chip (31) authorizes calculation (operation 5) only if the identifier stored in the storage means (32) of the chip (31) is in the list.

4. A cryptographic method according to any of claims 1 to 3, further comprising the following steps:

- at the same time as reading the list (operation 2), the chip (31) reads a signature in the list in the storage means of the second entity (operation 10), which signature was calculated beforehand by calculation means of the second entity, and

- before the chip (31) authorizes calculation by the calculation means (33) (operation 5), it verifies the validity of the signature (operation 11).

5. A cryptographic method according to either claim 1 or claim 2, further comprising the following steps:

- at the same time as reading the list (operation 2), the chip (31) reads the signatures of the identifiers in the list in the storage means of the second entity (operation 12), each identifier having given rise to a signature calculated beforehand by calculation means of the second entity,

- at the same time as reading the list (operation 2), the chip (31) reads in the storage means of the second entity a value of the number of identifiers listed in that list and a signature for that value (operations 13, 14), the value and its signature having been calculated beforehand by calculation means of the second entity,

- before the chip (31) authorizes calculation by the calculation means (33) (operation 5), it verifies the validity of each of the signatures (operations 16, 17),

- the chip (31) counts the number of identifiers contained in the read list (operation 15), and

- before the chip (31) authorizes calculation by the calculation means (33) (operation 5), it verifies that the value of the counter and the read value are the same (operation 18).

6. A smart card (30) for implementing a method according to any of claims 1 to 5, characterized in that the smart card (30) is equipped with a chip (31) which comprises:

- storage means (32) for storing a secret key and an identifier of a first entity that is a proprietor of the smart card,

- calculation means (33) adapted to execute a cryptographic algorithm whose input arguments include the secret key,

- means (34) for reading a list of identifiers in complete form in storage means of a second entity via a telecommunications network, and

- means (35) for authorizing calculation by the calculation means (33) as a function of the result of comparing the identifier and the contents of the list.